REMARKS

Applicants respectfully traverse and request reconsideration.

Claim 27 has been amended to correct a typographical error.

Claims 8, 11-15, 24, and 27-30 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Perlman et al. in view of Risch. In the "Response to Arguments" section of the Office Action, it appears that previous arguments by Applicant and specific claim language in addition to the specific teachings of the references may have been misapprehended. Applicants respectfully submit that the Perlman reference teaches an opposite approach to that claimed by Applicant and that even for arguments sake, combines the teachings of Risch would effectively make the mechanism in Perlman inoperable. Applicants also respectfully reassert the relevant remarks made in the previous response.

The Perlman reference is directed to a certification authority that issues a blacklist having a start date, and expiration date, and an entry for every invalid certificate issued after the start date. The Perlman certificates do not need expiration dates. The blacklist is a global list of all subscriber's invalid certificates issued after a start date. A new blacklist is issued prior to expiration of the current one and the blacklist start date is changed only when the black list becomes unmanageably long. (See for example Abstract). In fact, there is no expiration date used in the certificates of Perlman so that periodic certificate renewals is avoided. (See col. 3, lines 68 to col. 4, line 4). Instead, the blacklist as taught in Perlman has a start date and an expiration date and any certificates issued prior to the start date are automatically considered invalid. The blacklist of Perlman appears to simply be a list of only revoked or invalid certificates, none of which appear to be selectively chosen by an end user nor selectively evaluated by the server based on an update request from a user. Perlman does not contemplate

any type of monitoring by the server, changes that occur to public key certificates that were identified in the user request which included associated public keys or a certificate of a party that the end user was interested in. This is because Perlman appears to provide a conventional prior art mechanism for globally indicating expired certificates of many participants in the public infrastructure. The Perlman CA issues a new blacklist with a new expiration date but will usually keep the same start date and therefore will contain the same invalid certificates as in the previous list, plus any additional certificates that have been invalidated since the printing of the previous list. (See for example col. 6, lines 65 to col. 6, line 4). Only when the blacklist becomes to long to be conveniently managed is a new start date selected.

From a users perspective, the blacklist appears to be viewed like any other certificate revocation list for example. As noted, for example on col. 7, a user searches the blacklist for the certificate of another user. If the certificate is found in the blacklist, the certificate is considered to be invalid. If the certificate is not in the blacklist, it is assumed to be valid. As such, the blacklist contains certificates of many users in the system and cannot generate it in response to a certificate update subscription information from an end users nor is there monitoring of the certificate of a subscriber identified by the update subscription information according to Perlman as Perlman teaches an opposite approach. In fact, the blacklist in Perlman only appears to be updated when it becomes unreasonably long or when the blacklist's expiration date is approaching. There is no update to the blacklist performed based on, for example, an update subscription from an end user as such an operation is not contemplated by Perlman. Applicants respectively submit that Perlman teaches away from Applicant's claimed invention by teaching, for example, a global blacklist that is only updated for example, when the list becomes too long and independent of the generation of a certificate update subscription information. As such,

Perlman's combination with another reference such as Risch cannot render the claimed invention obvious as Perlman describes a completely different system from that claimed.

Also, as admitted in the Office Action, Perlman does not provide a facility for monitoring a specific public key certificate in response to update subscription information that is generated by an end user, nor receiving this certificate update subscription information from the user nor for notifying the user when it changes.

Since the Perlman reference does not teach or suggest these operations, it appears that the Risch reference is cited as describing these elements are not taught in Perlman. However, the Risch reference is directed to a method of monitoring changes in an object oriented database with tuned monitors and is not directed to public key certificate processing.

For arguments sake, even if the teachings of Risch were somehow properly combinable, such a combination would appear to contradict the fundamental operation of Perlman and render Perlman's system inoperative. For example, Perlman teaches that a main benefit of his system is that the blacklist need not be generated as often as other systems and it removes the need for expiry periods on certificates of participants in a system. Combining Risch, as best understood, with the teaches of Perlman would result in a system of Perlman that apparently that would require the blacklist to be updated every time a end user requested it to be updated which is in complete contradiction to the teachings of Perlman. Accordingly, Applicants respectfully submit that the teachings of Risch are not properly combinable with the teachings of Perlman.

Among other advantages, the claimed invention can provide end users, in real time, updates to public key certificates of subscriber subjects of interest to them. Thus, the information that an end user receives is only information that is relevant to the end user. In prior systems, such as that taught in Perlman, an end user would receive a certificate revocation list

(e.g. a type of blacklist) that would include thousands of entries wherein only a small percentage of the list would be of interest to the end user. (See for example Specification page 12, lines 10-15). Accordingly, claims 8, 11-15, 24, 27-30 are believed to be in condition for allowance.

As to claims 11 and 27, 12 and 28, Applicants respectively submit that these claims are allowable at least as depending from allowable base claim and as adding additional novel and nonobvious subject matter.

Accordingly, Applicants respectfully submit that the claims are in condition for allowance, and that an early Notice of Allowance be issued in this application. The Examiner is invited to contact the below-listed attorney if the Examiner believes that a telephone conference will advance the prosecution of this application.

Respectfully submitted,

Date: 12-23-04

By: _____
Christopher J. Reckamp
Registration No. 34,414

Vedder, Price, Kaufman & Kammholz, P.C.
222 North LaSalle Street
Chicago, Illinois 60601
Phone: (312) 609-7599
Fax: (312) 609-5005